Merja Aarnivuo-Seppinen

SIEM ulkoistettuna palveluna Case: Julkishallinto

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

05.05.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Merja Aarnivuo-Seppinen SIEM ulkoistettuna palveluna Case: Julkishallinto 39 sivua + 1 liitettä 05.05.2014
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Kari Järvi Tietoturva-asiantuntija Outi Juntura

Tässä opinnäytetyössä tarkastellaan SIEM-ratkaisun hankkimista ulkoistettuna palveluna julkisen hallinnon näkökulmasta. Työ on pyritty pitämään sellaisella tasolla, että siitä olisi hyötyä järjestelmän hankkijalle, vaikka hänellä ei olisi syvällistä SIEM-osaamista.

SIEM-järjestelmän hankinnan ja käyttöönoton määrittelyssä on monta huomioon otettavaa asiaa. Onnistunut SIEM-ratkaisun hankinta vaatiikin tarkkaa suunnittelua ja paljon etukäteistyötä, jotta hankinta vastaisi sille asetettuja tavoitteita. Hankinnalle asetettavien tavoitteiden määrittely on avainasemassa hankinnan onnistumiselle.

Julkishallinnon puolella ennen hankintaa tehtyjen määrittelyjen merkitys hankinnan onnistumiselle on erityisen suuri, koska hankinnan täydentäminen jälkikäteen voi osoittautua sekä haastavaksi että hinnakkaaksi. Järjestelmän hankkiminen ei kuitenkaan yksin riitä, vaan käyttöönoton ja käytön onnistuminen vaatii lisäksi myös suunnitelmallisuutta, resursseja, osaamista ja pitkäaikaista sitoutumista sekä palvelun jatkuvaa kehittämistä.

Työssä ei pyritty saamaan aikaan täydellistä listaa siitä, mitä kaikkea palvelun ulkoistajan tulee huomioida mutta työn avulla ostajalla on paremmat mahdollisuudet hahmottaa asiaan liittyvä kokonaisuus. Lopputyön tuloksena syntyi dokumentti, jota ulkoistetun SIEM-ratkaisun hankkija voi käyttää apunaan sekä tarvittavan ratkaisun määrittelyssä että hankittavan kokonaisuuden hahmottamisessa. Vaikka SIEM-ratkaisu hankitaan ulkoistettuna palveluna, kaikkea ei voi ulkoistaa, vaan myös tilaajaorganisaatiolle jää tehtäviä hoidettavaksi.

Avainsanat	SIEM, SIM, SEM, tietoturva, lokien hallinta

Author(s) Title Number of Pages Date	Merja Aarnivuo-Seppinen Outsourced SIEM-solution. Case: Public sector 39 pages + 1 appendices 05 May 2014
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Kari Järvi, Principal Lecturer Outi Juntura, Information Security Specialist

This thesis is about buying an outsourced SIEM solution in the public sector. The aim was to keep the study at such a level that it can be useful to a buyer who does not have that much experience with SIEM.

Making specifications for buying and implementing the SIEM system is not that easy and one needs to take many issues into account in order to get a successful result. To buy and implement the SIEM solution in such a way that it meets the requirements successfully one needs to plan everything carefully and do lots of work beforehand. Getting the specifications right is critical in order to get a working solution.

At the public sector the predefined specification is even more important because making changes afterwards can be extremely challenging and expensive. Buying the system is not enough if the plan is to have a truly working SIEM solution. One also needs to have orderliness, resources, know-how and long term commitment and readiness to continuously develop the solutions.

The present study is not about getting a complete list about what one should take into consideration while outsourcing the SIEM solution but to help the buyer to have better chances to piece together and see the entity. The outcome of the study is a document that can be used while specifying the solution needed and putting together the complexity of the SIEM solution. Even if the SIEM solution is bought as an outsourced service one cannot outsource everything, it is still necessary for the acquisition to take charge of some of the activities.

Keywords	SIEM, SIM, SEM, log management, information security

Sisällys

Lyhenteet ja sanasto

APT	Advance Persistent Threat. Kehittynyt pysyvä uhka.
COBIT	The Control Objectives for Information and related Technology. Hallintotavan malli IT-palvelujohtamiseen.
GRC	Governance, Risk and Compliance. Hyvän hallintotavan mukainen riskien ja vaatimusten hallintajärjestelmä.
IDS	Intrusion Detection System. Hyökkäyksen havaitsemisjärjestelmä.
IPS	Intrusion Prevention System. Hyökkäyksen estojärjestelmä.
ISO	International Organization for Standardization. Kansainvälinen standardointijärjestö.
ITIL	Information Technology Infrastructure Library. Kokoelma käytäntöjä IT-palveluiden hallintaan ja johtamiseen.
KATAKRI	Kansallinen turvallisuusauditointikriteeristö.
PCI DSS	Payment Card Industry Data Security Standard. Maksukorttialan tietoturvastandardi.
SEM	Security Event Management. Tietoturvatapahtumien hallinta.
SIEM	Security Information and Event Management. Tietoturvainformaation ja -tapahtumien hallinta.
SIM	Security Information Management. Tietoturvainformaation hallinta.
VAHTI	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä.
Poikkeama	Ero normaalitilanteeseen.
Häiriö	Tilapäinen haitta tai keskeytys.

1 Johdanto

Onnistunut SIEM-ratkaisun toteutus vaatii tarkkaa suunnittelua ja paljon etukäteistyötä, jotta lopputulos vastaisi sille asetettuja tavoitteita. SIEM-ratkaisun hankinnan ja käyttöönoton määrittelyssä on monta huomioon otettavaa asiaa, vaikka kokonaisuus hankittaisiinkin ulkoistettuna palveluna. Hankinnalle asetettavien tavoitteiden määrittely on avainasemassa lopputuloksen onnistumisen kannalta. SIEM-ratkaisua hankkiva organisaatio on usein tekemässä ensimmäistä SIEM-hankintaansa, eikä riittävää kokonaiskuvaa huomioonotettavista asioita ehkä kyetä muodostamaan. Tämän seurauksena voidaan päätyä tilanteeseen, jossa hankittu SIEM-ratkaisu ei täytäkään tilaajaorganisaation tarpeita. Palvelun hankkijan tulisi lisäksi pystyä varmistumaan siitä, että tilattu ja saatu palvelu vastaavat toisiaan.

Tämän opinnäytetyön tarkoituksena on auttaa hahmottamaan hankittavaa kokonaisuutta sekä mitä seikkoja tulisi ottaa huomioon, kun tehdään ulkoistetun SIEM-ratkaisun hankinnan määrittelyä ja käyttöönottoa. Työ pohjautuu julkisesti saatavilla olevaan materiaaliin sekä omassa työssä hankittuun tietoon ja kokemukseen.

1.1 Työn kattavuus

SIEM-järjestelmän hankinta lähtee liikkeelle tarpeen tunnistamisesta ja etenee määrittelyjen ja hankinnan eri vaiheiden kautta toteutukseen asti. Kuvassa 1 on kuvattu karkealla tasolla hankinnan päävaiheet.

Kuva 1. Hankinnan vaiheet

Tässä opinnäytetyössä käydään läpi muiden vaiheiden, paitsi varsinaisen hankinnan ja siihen sisältyvän SIEM-ratkaisun kilpailutuksen, hankinnan onnistumisen kannalta eri-

tyistä huomiota vaativat kohdat. Työssä ei ole tarkoitus ohjeistaa, miten näihin liittyvät prosessit tulisi hoitaa, vaan tarkoituksena on keskittyä löytämään vastauksia erityisesti seuraaviin kysymyksiin:

- Mikä on SIEM?
- Mihin SIEM-järjestelmää tarvitaan?
- Miten tarvittava SIEM-ratkaisu määritellään?
- Mitä ulkoistamiseen liittyviä asioita tulee huomioida?
- Mitä asioita pitää huomioida palvelun käyttöönotossa?
- Mistä asioista tulee sopia palvelun tuottajan kanssa?
- Mitä prosesseja tilaajaorganisaatioon tarvitaan, kun palvelu on ulkoistettu?

Opinnäytetyössä tarkastellaan hankintaa julkishallinnon näkökulmasta, mutta tässä esitetyt asiat ovat suurelta osin sovellettavissa myös muuhun kuin julkishallinnon tekemään hankintaan. Toinen työtä ohjaava näkökulma on hallinnollisen tietoturvan vaatimukset. Opinnäytetyö on tehty tilaajaorganisaation näkökulmasta. Työ on pyritty pitämään sellaisella tasolla, että siitä olisi hyötyä järjestelmän hankkijalle, vaikka hänellä ei olisi syvällistä SIEM-osaamista.

1.2 Työn rajaukset

Työssä keskitytään kokonaiskuvan muodostamiseen tarvittavan ratkaisun hankinnassa ja käyttöönotossa eikä työssä ole tarkoitus mennä tarkkoihin yksityiskohtiin. Työssä ei pyritä saamaan aikaan täydellistä listaa siitä, mitä kaikkea erityisesti ulkoistetun SIEM-ratkaisun hankkijan tulee huomioida, mutta työn avulla ostajalla on paremmat mahdollisuudet hahmottaa asiaan liittyvä kokonaisuus, jolloin myös SIEM-ratkaisun hankkimisen onnistumisen todennäköisyys kasvaa. Työssä ei ole tarkoitus vertailla eri valmistajien SIEM-järjestelmiä eikä siinä oteta kantaa eri toimittajien järjestelmien kattavuuteen, toimintaan tai käytettävyyteen. Työssä ei myöskään ole tarkoitus ottaa kantaa siihen, mitä lokeja kannattaisi kerätä tai miten SIEM-järjestelmä tulisi konfiguroida.

2 Mikä on SIEM?

SEM (Security Event Management) -järjestelmän avulla voidaan seurata siihen liitettyjen järjestelmien tapahtumia reaaliaikaisesti. Järjestelmä mahdollistaa nykyhetken monitoroinnin, ajantasaisen tapahtumien korreloinnin sekä nopeat automaattiset vasteet ennalta määriteltyihin tapahtumiin. SIM (Security Information Management) -järjestelmä puolestaan tarjoaa näkymää nykyhetkestä taaksepäin. SIM-järjestelmä tarjoaa kerätyille lokitiedoille pitkäaikaista varastointia ja tallennettuihin lokitietoihin perustuvaa tietojen analysointia, korrelointia ja raportointia. Järjestelmää, jossa on sekä SEM- että SIM-järjestelmien ominaisuudet samassa paketissa, kutsutaan SIEM-järjestelmäksi. [13; 19; 21.] SIEM-järjestelmän toteutuksessa keskitytään usein ensin SIM-järjestelmän osuuteen ja vasta sen onnistuneen toteutuksen jälkeen SEM-järjestelmän sisältämiin ominaisuuksiin. [13.]

SIEM-järjestelmän käytön tarkoituksena on kerätä useista lähteistä saadut lokit yhteen paikkaan sekä automatisoida eri järjestelmistä kerättyjen lokien käsittelyä mahdollisimman paljon. SIEM-järjestelmä myös muokkaa eri muodossa olevan datan käsiteltävämpään muotoon. SIEM-järjestelmän avulla voidaan taata lokien luottamuksellisuus, eheys, saatavuus ja kiistämättömyys sekä rajoittaa pääsy dataan pienelle käyttäjäjoukolle.

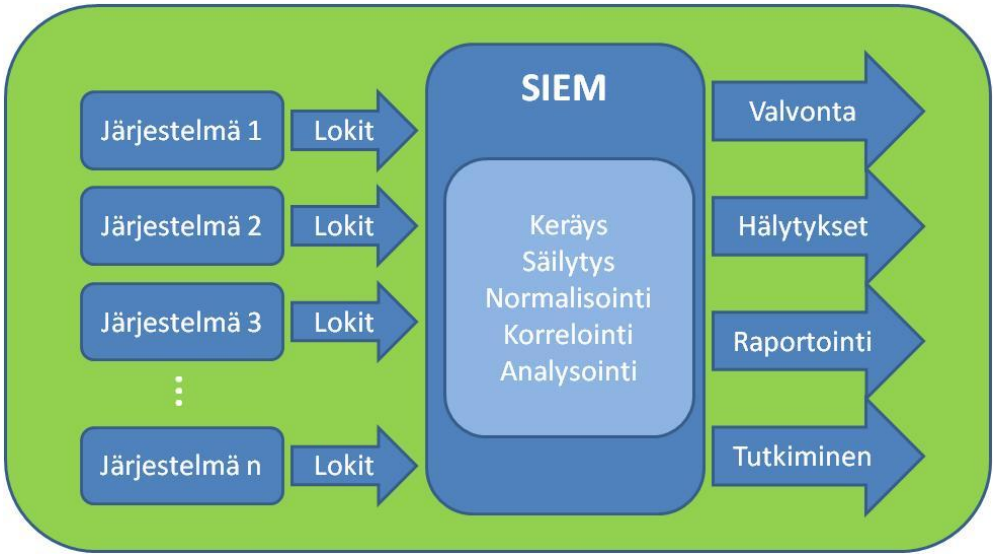
SIEM-järjestelmän avulla on mahdollista muodostaa sekä ajantasaista että historiatietoon perustuvaa kokonaistilannekuvaa organisaation käyttöön. SIEM-järjestelmä sisältää useita työkaluja päivittäisten lokitietojen ja tietoturvatapahtumien käsittelyyn. SIEM-järjestelmään voidaan valmistajasta ja ratkaisusta riippuen rakentaa erilaista analytiikkaa, esimerkiksi asettaa hälytysrajoja yhden järjestelmän poikkeaville tapahtumille tai yhdistää useammasta järjestelmästä kerättyjä tietoja yhteen raporttiin tai hälytykseen. Yhdistelemällä eri lähteistä saatavia tietoja voidaan helpommin havaita sellaisia tietoturvauhkia, joita ei voitaisi tunnistaa pelkästään yhdestä järjestelmästä saatavan tiedon perusteella, mutta jotka on mahdollista tunnistaa useasta lähteestä kerättyjen tietojen yhdistelmän muodostaman hyökkäyskuvion perusteella. SIEM-järjestelmän käytöllä voidaan parantaa tietoturvahenkilöstön mahdollisuuksia havaita mahdolliset epäilyttävät tapahtumat aikaisemmin, jolloin niihin voidaan reagoida nopeammin ja siten pienentää poikkeamasta aiheutuvaa haittaa.

Kuva 2. SIEM-ratkaisu

SIEM-järjestelmän käyttö vaatii osaavaa henkilökuntaa, jotta järjestelmä toimisi oikein ja siitä saataisiin mahdollisimman suuri hyöty. Tässä opinnäytetyössä SIEM-ratkaisulla tarkoitetaan kokonaisuutta, joka muodostuu sekä tarvittavasta järjestelmästä että sen päälle rakennetusta, ihmisten tuottamasta palvelusta.

3 Mihin SIEM-ratkaisua tarvitaan?

SIEM-järjestelmän hankinnalle tulee aina olla liiketoiminnasta johdetut perusteet. Keskitetty tietoturvainformaation ja -tapahtumien hallintajärjestelmä parantaa yrityksen mahdollisuuksia toimia oman tietoturvapolitiikkansa mukaisesti ja sen avulla voidaan tarvittaessa osoittaa toiminnan viitekehysten (kuten PCI DSS, COBIT, ITIL tai ISO) vaatimustenmukaisuus.



Kuva 3. SIEM-periaate

Lokit ovat osa järjestelmän tietoturvallisuuden valvontaa sekä tietojärjestelmien ylläpitoa. SIEM-järjestelmään kerättyjen lokien avulla saadaan ajantasaista kokonaiskuvaa järjestelmien tilanteesta, voidaan valvoa järjestelmiä, tuottaa tarvittavia raportteja sekä tunnistaa erilaisia poikkeamia ja häiriöitä sekä reagoida niihin. Lokitietojen keräyksen avulla voidaan myös varmistaa järjestelmää käyttävien henkilöiden oikeusturvaa, samoin kuin niiden henkilöiden, joiden henkilötietoja on järjestelmissä, joista lokitietoja kerätään. Lokeista tuotettu näyttö tapahtumasta voi joko tukea tai kumota luvattoman käsittelyn epäilyjä, mikäli lokitiedot on kerätty ja säilytetty oikein. [5;22.]

3.1 Kokonaiskuvan muodostaminen

Keskitettyyn lokien keräykseen liitetyistä järjestelmistä voidaan muodostaa ajantasaista kokonaiskuvaa helpommin, kuin jos sama tieto pitäisi kerätä pala kerrallaan eri lähteistä. Kertyvän tiedon perusteella syntyy käsitys siitä, mikä on eri järjestelmien normaalitilanne. Kun normaalitilanne tunnetaan, siitä poikkeavien tilanteiden havaitseminen on helpompaa. Normaalitilanteen tuntemista voidaan hyödyntää esimerkiksi arvioitaessa oikeita raja-arvoja erilaisille hälytyksille. [22.]

3.2 Valvonta ja raportointi

Lokien sisältämä tieto on usein hyödytöntä, jollei sitä saada ymmärrettävämpään muotoon. SIEM-järjestelmän käyttö helpottaa lokien sisältämän tiedon saamista paremmin ymmärrettävään muotoon mm. hälytyksiksi ja raporteiksi. Hälytyksiä ja tuotettuja raportteja voidaan käyttää hyväksi järjestelmien valvonnassa. Hälytysten perusteella voidaan tehdä joko manuaalisia toimenpiteitä, tai ne voivat johtaa automatisoituihin toimenpiteisiin. Raporttien avulla lokien sisältämät merkinnät saadaan helpommin luettavaan ja ymmärrettävään muotoon, jolloin mahdollisten toimenpiteitä vaativien tapahtumien havaitseminen helpottuu. Raporttien avulla voidaan mm. havaita suorituskykyongelmia, järjestelmään tunkeutumisia, yhteiskäyttöisien tunnuksien käyttöä tai konfiguraatiovirheitä ja valvoa pääsyä tietoihin.

Raporttien muodostaminen on nopeaa, koska SIEM-järjestelmässä raporttien ja valvonnan tarvitsemat tiedot saadaan yhdestä paikasta sen sijaan, että tiedot haettaisiin ensin kustakin laitteesta ja yhdistettäisiin manuaalisesti. Raporttiin voidaan myös hel-

posti koota useasta eri lähteestä kerättyjä tietoja. Lisäksi järjestelmistä syntyy niin paljon lokeja, että niiden hallinta ja käsittely manuaalisesti ei ole enää käytännössä mahdollista, koska päivittäin syntyvän lokitiedon määrä on suurempi kuin mitä manuaalisesti samassa ajassa ehdittäisiin käsittelemään.

Raportteja voidaan käyttää paitsi järjestelmän tilan valvomiseen myös osoittamaan organisaation toiminnan vaatimustenmukaisuuden täyttyminen. SIEM-järjestelmät tarjoavat usein valmiita raporttimalleja, joiden avulla vaatimusten täyttyminen voidaan osoittaa esimerkiksi auditoijalle.

3.3 Reagointikyvyn parantaminen

SIEM-järjestelmän avulla on mahdollista saada aikaan ajantasaista kokonaiskuvaa järjestelmien tilanteesta. Muodostetun tilannekuvan avulla voidaan nopeuttaa poikkeavien tilanteiden havaitsemista.

Havaittuihin tietoturvatapahtumiin voidaan reagoida, toisin kuin niihin, jotka jäävät havaitsematta. KPMG Oy Ab:n 15.1.2014 julkaiseman tutkimuksen ”Unknown Threat in Finland” [1.] mukaan noin puolessa tutkimuksessa mukana olleista yrityksistä oli nähtävissä merkkejä aktiivisista tietomurroista, joita käytössä olleet suojausmekanismit eivät olleet pystyneet estämään. SIEM-järjestelmien avulla voidaan helpommin havaita myös esimerkiksi APT (Advance Persistent Threat) -tyyppinen hyökkäys. [2; 3.]

Tietomurtotapauksissa murtautuja yrittää usein ensimmäiseksi lamauttaa lokien keräämisen ja pyrkii pyyhkimään omat jälkensä pois lokeista. Tästäkin syystä lokitiedot tulee suojata asiattomilta muutoksilta ja ne tulee säilyttää siten, ettei niitä voida jälkikäteen muuttaa. Nopeammalla reagoinnilla pystytään pienentämään häiriöistä ja poikkeamista aiheutuvia vahinkoja. [4.]

3.4 Tapahtumien kulun selvittäminen

Tapahtuman tai tapahtumaketjun selvittämiseksi tarvittavien lokien kerääminen on yksinkertaisempaa ja nopeampaa, kun lokit voidaan hakea yhdestä järjestelmästä. Lokien avulla voidaan selvittää tapahtumien kulkua eri yhteyksissä, esimerkiksi virhe- tai vää-

rinkäyttötilanteissa sekä tietoturvatapahtumien selvittämisessä. Lokimerkintöjen avulla voidaan osoittaa tapahtuma ja sen osapuolet siten, ettei tapahtumaa tai osallisuutta tapahtumaan voida kiistää. Lokien avulla voidaan dokumentoida tapahtumien kulku keräämällä tiedot eri järjestelmien sisältämistä lokeista ja laittamalla ne aikajärjestykseen (audit trail). Tämä edellyttää, että lokeja tuottavien järjestelmien kellot ovat synkronoituja. Lokitietoja voi olla tarpeen käyttää myös todistusaineistona mahdollisessa oikeudenkäyntiprosessissa.

4 Tarpeen määrittely

Ennen hankintaa tulee selvittää, mihin tarkoitukseen SIEM-ratkaisua ollaan hankkimassa ja mitä tavoitteita hankinnalle on asetettu. Hankinta on saattanut alun perin lähteä siitä ajatuksesta, että hankkimalla SIEM-järjestelmä saadaan lainsäädännölliset vaatimukset täytetyksi tai tietoturvapolitiikan tavoitteiden täyttämiseksi käytössä pitää olla SIEM. SIEM-järjestelmä on kuitenkin hankintana hinnakas, ja jotta järjestelmästä saataisiin mahdollisimman paljon vastinetta rahalle, sen aiottu käyttö kannattaa suunnitella huolella ja huomioida myös sen käytön vaatima osaaminen.

Ennen kuin päätös SIEM-järjestelmän hankinnasta kannattaa tehdä, tulee paitsi tietää, mihin tarkoitukseen SIEM-järjestelmää ollaan hankkimassa, myös mitä ja missä muodossa olevia lokeja järjestelmistä syntyy ja miten lokeja tulisi käsitellä sekä mitä muita vaatimuksia ja tavoitteita lokien keräykselle ja käsittelylle on mahdollisesti asetettu. Tarvitsevatko jotkut lokit esimerkiksi erityisseurantaa tai erityistä käsittelyä? Erityisseurantaa ja erilaista käsittelyä vaativia lokeja voivat olla esimerkiksi pääsynvalvontaan liittyvät lokit, lokien käsittelyyn liittyvät lokit tai mahdolliset hankittavan SIEM-palveluntuottajan kilpailijan konesalissa olevat palvelimet.

SIEM-järjestelmän valintaan vaikuttavat myös siihen liitettävien järjestelmien asettamat tekniset vaatimukset mm. lokien keräyksen tai laitteistojen sijainnin suhteen. Palvelun toiminnan sekä siihen liitettyjen järjestelmien valvonta asettaa myös omat vaatimuksensa hankittavalle järjestelmälle ja palvelulle.

Kuva 4. Tarvittavan ratkaisun määrittely

Määrittelyn edetessä voidaan myös joutua palaamaan hankinnalle aiemmin asetettuihin tavoitteisiin ja täsmentämään niitä tarpeen mukaan. SIEM-järjestelmän avulla saatavaa hyötyä tulee myös arvioida suhteessa siitä aiheutuviin kustannuksiin.

4.1 Käyttötarkoituksen suunnittelu

Jokaiselle SIEM-järjestelmän käyttöönotettavalle asialle tai toiminnolle tulee määritellä käyttötarkoitus. Ilman ennakkoon mietittyä käyttötarkoitusta voidaan päätyä tilanteeseen, jossa esimerkiksi tuotetaan raporttia, jota kukaan ei lue ja joka ei koskaan voi johtaa mihinkään toimenpiteeseen. Jokaiselle käyttöönotetulle toiminnolle on paitsi nimettävä vastuutaho myös hankittava tarvittavat resurssit toiminnon toteuttamiseksi.

Kuva 5. SIEM-järjestelmän käyttötarkoituksen hahmottaminen

Käyttötarkoituksen hahmottamiseen karkealla tasolla voi käyttää apuna alla olevaa kysymyslistaa.

- Onko tarkoitus viedä SIEM-järjestelmään kaikki lokit vai esimerkiksi vain kriittisten järjestelmien lokit?
- Onko tarkoituksena turvata lokien käyttökelpoisuus ja saatavuus mahdollista väärinkäytöstä seuraavassa oikeudenkäynnissä vai riittääkö, että lokit ovat ylipäätään tallessa jossain?
- Onko tarkoituksena rajoittaa pääsyä lokeihin?
- Onko ensisijainen tarve lokien asianmukainen säilyttäminen vai onko painopiste esimerkiksi keräyksen päälle rakennettavassa raportoinnissa tai analytiikassa?
- Onko tarkoituksena seurata aktiivisesti ja reaaliaikaisesti järjestelmien tilannetta vai esimerkiksi suorittaa valvontaa vain päivittäin, viikoittain vai kuukausittain lokien perusteella muodostettavien raporttien avulla?
- Halutaanko SIEM-järjestelmässä yhdistää tai analysoida eri järjestelmistä saatavia tietoja (esim. IDS/IPS:stä, palomuurista tai virus- ja haittaohjelmista saatavia tietoja)?

- Tarvitaanko hälytyksiä ja automaattista reagointia etukäteen määriteltyihin tietoturvauhkiin tai muihin vastaaviin tilanteisiin? Tarvitaanko muunlaista reagointia?

Tietoturvanäkökulmasta lokien kiistämättömyys ja eheys ovat usein tärkeitä, koska mahdollinen hyökkääjä pyrkii usein poistamaan mahdollisuuksien mukaan hyökkäyksen jäljet lokeista sekä pysäyttämään lokituksen. Organisaation toiminnan tai sen tuottaman palvelun jatkuvuuden kannalta taas voi olla tärkeämpää ajantasaisen kokonaiskuvan muodostaminen järjestelmien tilasta sekä häiriöiden ja poikkeamien havaitseminen ja niihin reagoiminen nopeasti.

Jos tarkoituksena on vain kerätä lokit talteen eri järjestelmään, niin silloin voi riittää yksinkertaisempi järjestelmä, jossa on vähemmän analytiikkaa tai raportointimahdollisuuksia. SIEM-järjestelmien perusominaisuuksia ovat yleensä lokien säilyttäminen muuttumattomina sekä niiden säilymisen varmistaminen. Jos lokit viedään talteen esimerkiksi erilliselle palvelimelle, palvelimen on tarpeen kuulua varmistusten piiriin. Erillistä palvelinta käytettäessä lokien muuttumattomuutta ei todennäköisesti voida varmistaa. Lokien muuttumattomuuden varmistaminen voidaan hoitaa myös tallentamalla ne ns. read only -medialle. Read only -medialle tallennettua tietoa ei voi muuttaa. Tämän ratkaisun heikkona puolena on usein varmistusten puuttuminen.

Pääsy lokeihin ja niiden perusteella muodostettuun tietoon on usein tarpeen antaa vain rajatulle joukolle henkilöitä. Järjestelmän tulee siksi mahdollistaa tarkoituksen mukainen tehtävien eriyttäminen sekä tilaaja- että palveluntuottajan organisaatiossa.

Liitettävien järjestelmien määrä vaikuttaa mm. kertyvän lokin määrään. Liitettävien järjestelmän määrällä on myös vaikutusta järjestelmän hankinnasta ja käytöstä aiheutuviin kustannuksiin. Toisaalta, mitä enemmän järjestelmiä on ratkaisun piirissä, sitä laajempi tilannekuva voidaan muodostaa. Monet SIEM-järjestelmät mahdollistavat eri järjestelmistä kerättyjen tietojen yhdistämisen. Eri lähteistä kerätyt tiedot voivat yhdessä muodostaa tunnistettavan uhkakuvion, vaikka yksittäin kerättyjen tietojen perusteella uhkaa ei voitaisi tunnistaa.

Pelkkä SIEM-järjestelmän hankkiminen ei kuitenkaan auta esimerkiksi tietoturvauhkien torjuntaan vaan järjestelmän lisäksi tarvitaan osaavaa henkilökuntaa, joka hoitaa järjestelmän päivittäisen operoinnin lisäksi myös kokonaiskuvan muodostamisen ja reagoi havaintoihin niiden vaatimalla tavalla. Jos tarkoituksena on seurata järjestelmien tilan-

netta aktiivisesti päivittäin, niin seurantaa tekevällä henkilöstölle tulee olla pääsy järjestelmään. Mikäli ulkoistettu SIEM-ratkaisu tuotetaan ns. moniasiakasympäristössä, niin tilaajaorganisaatiolla ei välttämättä ole mahdollisuutta saada pääsyä järjestelmään, vaan pääsy järjestelmään voi olla vain palvelun tuottajaorganisaatiossa. Tämä mahdollinen rajoitus kannattaa huomioida mahdollisimman varhaisessa vaiheessa, koska sillä voi olla merkittävää vaikutusta, jos järjestelmää halutaan tulevaisuudessa kehittää tai sen käyttötarkoitusta halutaan muuttaa tilaajaorganisaatiossa.

Sen jälkeen, kun SIEM-ratkaisun käyttötarkoitus on saatu suunnitelluksi riittävällä tasolla, voidaan siirtyä tarkastelemaan, mitä muita vaatimuksia hankittavalle järjestelmälle asetetaan.

4.2 Tekniseen toteutukseen vaikuttavat tarpeet

Hankittavan SIEM-järjestelmän teknisellä toteutuksella on merkittävä vaikutus järjestelmän käytettävyyteen ja häiriönsietoon. SIEM-järjestelmän on tarkoitus pystyä vähintäänkin keräämään ja tallentamaan lokeja koko ajan. Häiriöttömän keräyksen vaatimus tulee huomioida järjestelmälle asetettavissa teknisissä vaatimuksissa. Käytännössä tämä tarkoittaa sitä, että valittavan järjestelmän salliman maksimi keräysnopeuden tulee olla riittävän suuri tarpeeseen nähden ja lokien keräämiseen tarvittavien komponenttien tulee olla jollakin tapaa kahdennettuja. Keräimissä tulee esimerkiksi olla riittävät välimuistimahdollisuudet alle vuorokauden mittaisten keräys- ja tallennuskatkosten varalle. Välimuistitoteutuksella varmistetaan, että kerättyjä lokeja ei menetetä katkon aikana ja että keräys toimii normaalisti keräys- ja tallennuskerrosten välisistä katkoksista huolimatta. Keskitettyyn lokienkeräysjärjestelmään liittyviä ohjelmistoja on myös tarpeen päivittää aika ajoin, joten olisi hyvä valita sellainen tekninen toteutus, jossa päivitysten lokikeräykselle aiheuttamia katkoja ei olisi lainkaan tai ne olisivat mahdollisimman lyhyitä ja harvoin tapahtuvia. Valittavan teknisen toteutuksen olisi hyvä mahdollistaa myös muiden huolto- ja ylläpitotöiden teko ilman, että niistä aiheutuu käyttökatkoksia tai niistä aiheutuvat käyttökatkokset ovat mahdollisimman lyhyitä.

Kuva 6. Esimerkkejä hankinnalle asetettavista teknisistä vaatimuksista.

SIEM-järjestelmään voidaan kerätä lokeja monista fyysisistä sijainneista ja IP-osoitteista, mikä tarkoittaa sitä, että SIEM-järjestelmän ja keräyksen kohteena olevien järjestelmien välille tarvitaan tietoliikenneyhteys. Tämä tietoliikenneyhteys tulisi voida toteuttaa mahdollisimman pienellä tietoliikenneavauksella, koska turhan laaja avaus heikentää verkon tietoturvaa. SIEM-järjestelmän teknisen ratkaisun olisi hyvä mahdollistaa lokien siirtoon käytettävien tietoliikenneyhteyksien suojaaminen ja salaaminen. Siirretyn tiedon eheydestä tulee myös voida varmistua.

Järjestelmän olisi hyvä tukea sekä agentillista että agentitonta keräystä. Agentillisessa keräyksessä keräyksen kohteena olevaan järjestelmään asennetaan keräysohjelmisto, joka kerää lokitiedot, normalisoi ne ja lähettää eteenpäin lokikeräimelle. Agentittomassa keräyksessä keräyksen kohde lähettää lokitiedon sellaisenaan lokikeräimelle. Lokitiedon normalisointi tehdään tässä vaihtoehdossa vasta lokikeräimellä. [24.]

Mikäli valitaan usean organisaation käytössä oleva järjestelmä, on huomioitava, että tällä ratkaisulla voi olla vaikutusta järjestelmän auditoitavuuden lisäksi myös siihen, minkälaisen pääsyn tilaajaorganisaatio voi saada järjestelmään sekä esimerkiksi siihen, miten koko järjestelmään vaikuttavat muutokset voidaan aikatauluttaa ja toteuttaa.

Järjestelmän fyysinen sijainti voi vaikuttaa esimerkiksi siihen, millaisia tietoja sinne voidaan tallentaa tai kuinka helposti tai vaikeasti ja millaisin kustannuksin järjestelmää voidaan auditoida. Valitulla teknisellä ratkaisulla voi olla vaikutusta myös siihen, miten itse SIEM-ratkaisun toimintaa voidaan valvoa ja kenen toimesta. Valittu tekninen ratkaisu voi vaikuttaa esimerkiksi siihen, kuinka helposti lokien keräyksen häiriöt havaitaan.

Osa SIEM-järjestelmän piiriin ajatelluista palvelimista voi olla virtualisoituja tai klusteroituja. Jos tällaisia järjestelmiä ei vielä ole, niin niitä voi olla tulevaisuudessa ja SIEM-järjestelmän tulisi mahdollistaa lokien siirto myös tällaisista ympäristöistä. Muutenkin ratkaisua valittaessa tulisi huomioida tulevaisuuden laajennustarpeet. Hankittavan järjestelmän teknisen ratkaisun tulisi sisältää tuotantoympäristön lisäksi erilliset testi- ja kehitysympäristöt.

SIEM-järjestelmät osaavat yleensä käsitellä suoraan erilaisia käyttöjärjestelmätason lokeja. Tilaajaorganisaatiolla on kuitenkin usein tarve siirtää keskitettyyn lokien hallintajärjestelmään myös sovellusten lokeja, joten on hyvä selvittää, minkälaisia lokeja järjestelmään voidaan siirtää suoraan ja millainen tuki on saatavissa sellaisille lokeille, joiden siirto SIEM-järjestelmään vaatii räätälöintiä järjestelmään. Järjestelmän tulisi pystyä käsittelemään tunnistamattomia ja normalisoimattomia lokeja.

4.3 Lokien elinkaaren määrittely

Lokien hallintaan ja jatkokäsittelyyn kohdistuvat vaatimukset ovat keskeisessä roolissa määriteltäessä tarvittavaa SIEM-ratkaisua. Lokien ja niiden sisältämän datan käsittelyyn liittyvien vaatimusten huolellinen määrittely on onnistuneen toteutuksen edellytys.

Kuva 7. Lokien käsittelystä syntyviä vaatimuksia

Lokimerkintöjen avulla voidaan osoittaa tapahtuma ja sen osapuolet siten, ettei tapahtumaa tai osallisuutta tapahtumaan voida kiistää. Lokien perusteella tapahtumista voidaan muodostaa tapahtumaketjuja (audit trail), joilla voidaan todentaa erilaisia tapahtumia. Lokien käsittely, koko niiden elinkaaren aikana lokien synnystä niiden tuhoamiseen asti, tulisi kuvata esimerkiksi lokisuunnitelmassa. Kuvauksessa tulisi olla mm. seuraavat asiat:

- Miksi lokeja kerätään?
- Mikä on lokien käyttötarkoitus?
- Mistä laitteista lokeja kerätään?
- Missä muodossa lokit ovat?
- Mikä on syntyvän lokin määrä?
- Sisältävätkö lokit henkilötietoja?
- Mikä on kunkin lokin suojaustarve?
- Missä lokia säilytetään?
- Kuka voi käsitellä lokeja?

- Mitä tarkoitusta varten lokeja voidaan käsitellä?
- Muodostetaanko lokeista raportteja? Jos muodostetaan niin mitä tarkoitusta varten ja kenen käyttöön?
- Kuinka pitkään kutakin lokia on tarpeen säilyttää
- Missä tilanteissa lokeja voidaan luovuttaa eteenpäin? Kuka voi antaa luvan lokien luovutukselle
- Miten lokien eheyttä valvotaan?

Nämä asiat voivat olla jo valmiiksi kuvattuina, mutta kuvauksen ajantasaisuus on syytä tarkistaa, koska kuvausta käytetään yhtenä merkittävänä lähtötietona SIEM-järjestelmän hankinnan määrittelyssä. Ilman asianmukaista kuvausta kerättävistä lokeista ja niiden elinkaaren hallinnasta on vaikeaa päätellä, tarvitaanko lokien hallintaan keskitettyä tietoturvainformaation ja -tapahtumien hallintajärjestelmää vai voidaanko lokeja säilyttää esimerkiksi pelkästään paikallisesti. Lokisuunnitelman perusteella voidaan määritellä, mitä vaatimuksia hankittavalle järjestelmälle tältä osin asetetaan. Lokisuunnitelman teon apuvälineenä voi käyttää esimerkiksi VAHTI 3/2009 -ohjetta. [5.]

4.3.1 Lokien käyttötarkoituksen määrittely

Ennen lokien keräämisen aloittamista tulee miettiä, miksi juuri tämä loki on tarpeen kerätä. Ylimääräisiä lokeja ei kannatta kerätä, koska jokaisen lokin asianmukaisesta säilyttämisestä aiheutuu kustannuksia. Vaikka kustannukset yksittäisen lokin kohdalla olisivatkin pienet, niin kaikkien lokien yhteenlaskettuna summana kustannus voi nousta hyvinkin suureksi. Toisaalta tarpeellisia lokeja ei tulisi jättää kustannusten pelossa keräämättä, koska keräämättä jättämisen seurausten kustannukset voivat helposti ylittää keräys- ja säilytyskustannukset. Jokaisen lokin kohdalla tulisikin tehdä arvio, tarvitaanko lokia vai ei.

Lokeja kerätään erilaisista tapahtumista erilaisia tarkoituksia varten, esimerkiksi

- järjestelmään tehtyjen muutosten seuraamiseksi
- sovellukseen tehtyjen muutosten seuraamiseksi
- sovellusten tapahtumien tallentamiseksi
- virhetilanteiden selvittämiseksi

- käytönvalvonnan toteuttamiseksi
- pääsynvalvonnan toteuttamiseksi
- väärinkäytösten jäljittämiseksi.

Lokin käyttötarkoitusta suunniteltaessa kannattaa miettiä, minkälaisia tapahtumia kyseisellä lokilla voitaisiin joutua todentamaan ja mitä tarkoitusta varten.

Lokien sisältämiä tietoja voidaan käyttää esimerkiksi erilaisiin valvontatarkoituksiin, raporttien muodostamiseen tai vaikkapa hälytysten pohjamateriaalina. Lokien käyttötarkoitusta päätettäessä tulee aina muistaa, että lokien käsittelyssä tulee huomioida vallitseva lainsäädäntö ja osa käyttötarkoituksista voi olla esimerkiksi työelämän tietosuojalain (759/2004) tai sähköisen viestinnän tietosuojalain (526/2004) perusteella kiellettyjä, eikä niitä voida siten toteuttaa. Osa käyttötarkoituksista, kuten lokin käyttäminen henkilöstön toimien tekniseen valvontaan, voi vaatia myös yhteistoimintalain (334/2007) mukaisen käsittelyn. Esimerkkejä lokien käyttöä sääteleviin lakeihin on listattu liitteessä 1. Lokien käyttötarkoituksen laillisuus kannattaakin tarkistuttaa alan asiantuntijalla, esimerkiksi lakimiehellä.

4.3.2 Lokeja sisältävät laitteet, lokitiedostojen tyyppi ja lokin määrä

Lokien keräyksen kannalta on oleellista tietää mistä kaikista laitteista lokeja tulisi kerätä ja missä laitteet fyysisesti sijaitsevat. Lokeja tuottavat palvelimet voivat sijaita fyysisesti laajalla alueella, ne voivat olla eri palveluntuottajien konesaleissa tai ne voivat olla useamman organisaation käytössä. Näistä syntyvät rajoitteet on tarpeen ottaa huomioon, kun suunnitellaan, mitä lokeja voidaan viedä hankittavaan SIEM-järjestelmään.

Se, missä muodossa syntyvät lokit ovat, vaikuttaa siihen, voidaanko aiotut lokit viedä SIEM-järjestelmään suoraan vai vaaditaanko niiden viemiseksi keskitettyyn tietoturvainformaation ja -tapahtumien hallintajärjestelmään räätälöintiä. SIEM-järjestelmän tulee myös kyetä normalisoimaan lokien sisältö, jotta niistä voidaan muodostaa tarvittavat raportit tai niiden päälle voidaan muodostaa haluttu analytiikka.

Arvioimalla kunkin lokin päivittäin syntyvää määrää saadaan käsitystä siitä, kuinka paljon tallennuskapasiteettia hankittavaan SIEM-järjestelmään tarvitaan, kun lokeja säilytetään lokisuunnitelmassa mainittu aika.

4.3.3 Lokien sisältämät henkilötiedot ja lokien suojaustarve

Lokin kerääjän tulee arvioida, sisältävätkö lokit henkilötietoja. Henkilötiedolla tarkoitetaan Henkilötietolain (HetiL 523/1999) 3 § mukaan ”kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi”. Lokien mahdollisesti sisältämät henkilötiedot vaikuttavat siihen, miten lokeja voidaan käsitellä ja missä niitä voidaan säilyttää.

Kunkin lokin sisältämän tiedon suojaustarve määritellään lokikohtaisesti. Suojaamista voidaan tarvita sekä tahattomasti että tahallisesti (esim. haittaohjelmat) tapahtuvan lokin muuttamisen varalle. Lokit tulee suojata myös asiatonta pääsyä vastaan. Kunkin lokin säilytystapa määräytyy suojaustarpeen mukaisesti ja loki tulee suojata siten, että sen eheys ja luottamuksellisuus säilyvät suojaustarpeen mukaisesti. Erityistä suojausta vaativia lokeja voisivat olla esimerkiksi pääsynvalvontaan tai lokien käsittelyn valvontaan liittyvät lokit.

4.3.4 Lokien säilytyspaikka ja -aika

Lokin saaminen käyttöön keskitetystä tietoturvainformaation ja -tapahtumien hallintajärjestelmästä saattaa viedä jonkin aikaa, joten osa lokeista voi olla tarpeen säilyttää jonkun aikaa palvelimella esimerkiksi mahdollista nopeaa vian selvitystä varten. Lokin kopio voi olla silti tarpeen siirtää suojaan keskitettyyn lokijärjestelmään.

Säilytyspaikkaa valittaessa tulee lisäksi huomioida, että henkilötietoja sisältävien lokien säilyttämispaikan sijaintiin voi kohdistua myös lainsäädännöllisiä vaatimuksia.

Lokien säilytysaika määräytyy pääsääntöisesti substanssin asettamien vaatimusten perusteella. Yleensä lokeja on tarpeen säilyttää jonkin viitekehyksen vaatima aika tai niin kauan, kun on mahdollista esittää jotain lokien sisältämiä tapahtumia koskevia oikeudellisia vaatimuksia.

4.3.5 Lokien käsittely ja käsittelyn tarkoitus sekä lokien luovuttaminen

Lokeja on tarpeen käsitellä esimerkiksi raporttien laatimiseksi, toiminnan analysoimiseksi, virhetilanteiden selvittämiseksi tai tilannekuvan muodostamiseksi. Osa lokien

käsittelystä on säännöllisesti tapahtuvaa ja osa tehdään tarpeen vaatiessa, esim. häiriön selvittämiseksi. Käsittelyn osalta tulee kuvata, kuka voi käsitellä lokeja mitäkin tarkoitusta varten ja missä yhteydessä.

Joissakin tilanteissa, esimerkiksi rikostutkinnan yhteydessä, lokeja voi olla tarpeen luovuttaa eteenpäin. Näiden tilanteiden varalle tarvitaan ennalta hyväksytyt prosessit, joiden mukaan tilanteissa toimitaan.

4.3.6 Lokien eheyden valvonta

SIEM-järjestelmän perusominaisuuksia on lokien eheyden säilyttäminen, mutta mikäli lokien siirto SIEM-järjestelmään ei ole reaaliaikaista, voi olla tarpeen valvoa lokien eheyden säilymistä niiden muodostumisen alkupisteessä. Lokien eheyttä voidaan valvoa erillisellä lokien käsittelylokilla, joka suojataan ylläpidon pääsyltä. Lokien eheyden valvomiseksi lokeissa voidaan lisäksi käyttää esimerkiksi tarkistussummaa..

4.3.7 Raporttien määrittely

Ennen hankintaa tulee miettiä, onko lokien perusteella tarkoitus tuottaa raportteja vai ei. Yleensä raportteja on tarpeen tuottaa valvonnan tarpeisiin sekä osoittamaan toiminnan vaatimusten mukaisuus esimerkiksi auditoijalle. Tuotettavista raporteista on tarpeen kuvata, mitä käyttötarkoitusta varten raportteja tullaan tuottamaan ja kuinka usein niitä on tarpeen saada sekä missä muodossa saatavien raporttien tulisi olla. Lisäksi tulisi miettiä, onko raportteja tarkoitus käsitellä manuaalisesti vai onko käsittely tarkoitus automatisoida, kuinka pitkään ja missä raportteja säilytetään ja kuka niitä saa käsitellä. Raporttien ja niiden käyttötarkoituksen määrittelyssä kannattaa käyttää asiantuntijoiden apua.

4.4 Palvelun tuottamisen ja toiminnan valvonta

SIEM-ratkaisun käyttö tarkoituksenmukaisella tavalla edellyttää että sekä itse SIEM-järjestelmä että siihen liittyvän palvelun toiminta on luotettavaa, valvottua sekä dokumentoitua. SIEM-järjestelmän tekninen ratkaisu sekä palvelun tuottamistapa vaikuttavat merkittävästi siihen, millaisia keinoja valvonnan toteuttamiseksi on saatavilla. Valvonnan toteuttaminen kannattaa suunnitella vähintään karkealla tasolla jo määrittely-

vaiheessa, jotta voidaan varmistua siitä, että valittavalla ratkaisulla voidaan saavuttaa tilaajaorganisaation kannalta riittävä valvonnan taso. SIEM-ratkaisun auditoitavuuden tarpeeseen tulee ottaa kantaa jo määrittelyvaiheessa.

5 Ulkoistamisen erityispiirteet

Tilaajaorganisaatiolla on vastuu omasta toiminnastaan myös silloin, kun palvelun tuottamista on siirretty organisaation ulkopuoliselle taholle. Ulkoistettaessa palveluita annetaan aiemmin organisaation sisällä pysynyttä tietoa organisaation ulkopuolisen toimijan haltuun. Toimintaa ulkoistettaessa ei kuitenkaan voida ulkoistaa vastuuta eikä siten valvontaakaan voida täysin ulkoistaa. Ulkoistettaessa SIEM-ratkaisuun liittyviä palveluita tai niiden osia, on syytä kiinnittää erityishuomiota tietojen luottamuksellisuuden säilyttämiseen eri tilanteissa sekä palvelun tuottamisen valvontaan. Tilanteet, joissa tietojen luottamuksellisuus erityisesti voisi vaarantua, kannattaa yrittää tunnistaa mahdollisimman hyvin etukäteen.

5.1 Tiedon luottamuksellisuus

Lokitiedot sekä niistä johdettavissa olevat tiedot sisältävät yleensä paljon luottamuksellisiksi katsottavia tietoja kuten verkon tai järjestelmien rakennetta koskevia tietoja tai sovellusten sisältämiä tietoja. Näiden tietojen tulee säilyä luottamuksellisina, vaikka ne siirrettäisiin ulkoisena palveluna tuotettuun keskitettyyn tietoturvainformaation ja -tapahtumien hallintajärjestelmään.

5.1.1 Pääsy dataan

SIEM-järjestelmän sisältämiin tietoihin tulisi tietoturvanäkökulmasta olla mahdollisimman harvalla pääsy, mutta jatkuvuuden kannalta kuitenkin riittävän monella, jotta järjestelmän sisältämät tiedot saadaan käyttöön silloin, kun niitä tarvitaan. Jos tietoihin pääsee liian harva, on mahdollista, että tarvittavien tietojen saanti jopa estyy esimerkiksi lomien aikana tai sairastumisen seurauksena tai näiden yhdistelmän sattuessa. Jos pääsy on liian suurella joukolla, riskinä taas on lokitietojen tai niistä muodostettujen raporttien leviäminen liian laajalle joukolle. Erityissijaisjärjestelyistä syntyy yleensä yli-

määräisiä kustannuksia ja niillä saavutettu hyöty tulisi arvioida suhteessa aiheutuneisiin kustannuksiin.

Palvelinten ylläpitäjillä voi myös käytännössä olla pääsy dataan, jollei tätä pääsyä erikseen teknisesti estetä. Tämä voi esimerkiksi tapahtua rajoittamalla ylläpidon oikeuksia sekä itse palvelimille että lokit sisältävään tietokantaan. Mikäli ylläpidon oikeuksia ei ole rajoitettu tai SIEM-järjestelmän ylläpitoa tekevien henkilöiden ryhmää ei ole rajattu, niin huonoimmassa tapauksessa kaikilla ulkoistetun palvelun tuottajan palvelinten ylläpitoon osallistuvilla henkilöllä saattaa olla pääsy palvelimille ja siten mahdollisuus esimerkiksi kopioida lokien sisältö muuta käyttötarkoitusta varten. Lokien hallinnoijien tehtävät tulee erottaa infran ylläpitotehtävistä, eikä sama henkilö voi tehdä molempia tehtäviä.

Ulkoistettuna tuotettua palvelua voidaan tuottaa myös muualta kuin Suomesta ja palvelun ostajan tulee arvioida, voidaanko keskitetty tietoturvainformaation ja -tapahtumien hallintapalvelu tuottaa mistä maasta tahansa vai tuleeko tälle palvelulle asettaa jotain rajoituksia tuotantomaan suhteen lokien sisältämän datan perusteella jo kilpailutusvaiheessa. Asetettavien tuotantomaata koskevien rajoitusten tulee julkisella sektorilla yleensä perustua tilaajaorganisaation toimintaa koskevaan lainsäädäntöön.

5.1.2 Pääsy raportteihin

Ulkoistetun palvelun tuottajalla voi olla pääsy kerätyistä lokeista muodostettaviin raportteihin. Raporttien tuottaminen voi myös olla määritelty palvelun tuottajan tehtäväksi, jolloin ostajalla ei välttämättä ole lainkaan suoraa pääsyä raportteihin vaan raportit saadaan vain sovittuina ajankohtina toimitettuina. Tilaajan tuleekin miettiä, millainen pääsy raportteihin tarvitaan, riittävätkö esimerkiksi kuukausittain toimitettavat raportit vai tulisiko tilaajan voida tuottaa raportteja itse suoraan järjestelmästä.

Ulkoistettuna tuotettua palvelua voidaan tuottaa myös muualta kuin Suomesta ja palvelun ostajan tulee arvioida, voidaanko lokien raporttien tuottaminen hoitaa mistä maasta tahansa vai tuleeko tälle palvelulle asettaa jotain rajoituksia tuotantomaan suhteen raporttien sisältämän datan perusteella jo kilpailutusvaiheessa. Palvelinten ylläpitäjillä voi myös käytännössä olla pääsy raportteihin, jollei tätä pääsyä erikseen teknisesti estetä eriyttämällä lokien hallintajärjestelmä verkkotasolla muusta infrasta. Lisäksi sama henkilö ei voi tehdä sekä ylläpitotehtäviä että lokien hallinnointia.

5.1.3 Lokien siirtotapa

Tilaajan tulee hankintaa tehdessään määritellä, voidaanko järjestelmistä kerätyt lokit siirtää eteenpäin keskitettyyn lokienhallintajärjestelmään selväkielisinä vai pitääkö siirtoyhteyden ja/tai siirrettävän aineiston olla suojatussa muodossa. Vaikka tietoliikenneyhteydet olisivat sisäverkossa, niin siirtoyhteydet olisi hyvä suojata ulkopuoliselta pääsyltä. Suojaamisen merkitys kasvaa entisestään, jos lokien siirto keskitettyyn lokienhallintajärjestelmään edellyttää julkisen verkon käyttöä tai jopa tiedonsiirtoa toiseen maahan.

5.2 Valvonta

SIEM-järjestelmän hankkiminen ulkoistettuna palveluna ei vapauta hankkijaa valvontavastuusta. Ostajan on laadittava suunnitelma valvonnan periaatteista ja toteuttamistavasta sekä valvottava, että palvelua kokonaisuudessaan tuotetaan sovittuja toimintatapoja noudattaen, myös silloin jos palvelua tuotetaan ulkomailta. Ostajan tulee myös huolehtia siitä, että palvelun tuottamiseksi tarvittavat tehtävät on eriytetty siten, ettei hallitsemattomia vaarallisia työyhdistelmiä synny.

Yhtenä keinona järjestelmän toiminnan oikeellisuuden valvonnassa voidaan käyttää auditointia, joka voi olla ostajan, palvelun tuottajan tai kolmannen osapuolen tekemä. Auditointien osalta on sovittava mm. kuinka usein ja millä tavalla auditoinnit voidaan toteuttaa sekä miten niistä syntyvät kustannukset tullaan jakamaan. Ajoittain tehtävä auditointi on hyvä lisäkeino jatkuvan valvonnan rinnalla, mutta sillä ei voida korvata jatkuvaa valvontaa.

5.3 Tarvittava henkilötyömäärä

Keskitetyn tietoturvainformaation ja -tapahtumien hallintajärjestelmän hankkiminen, käyttöönotto ja käyttö tulevat vaatimaan henkilötyötä paitsi palveluntuottajalta myös ostajan puolelta. Osa tarvittavista resursseista voidaan hankkia ostopalveluina, mutta järjestelmän käyttöönotto ja käyttö tulevat vaatimaan myös ostajan omia resursseja. Palvelun jatkuvaan tuottamiseen tarvitaan osaavaa henkilökuntaa paitsi itse laitteiston käyttöön ja ylläpitoon myös mm. poikkeamiin reagoimiseen, raporttien tulkitsemiseen ja kokonaiskuvan muodostamiseen sekä järjestelmän kehittämiseen, muutosten hallin-

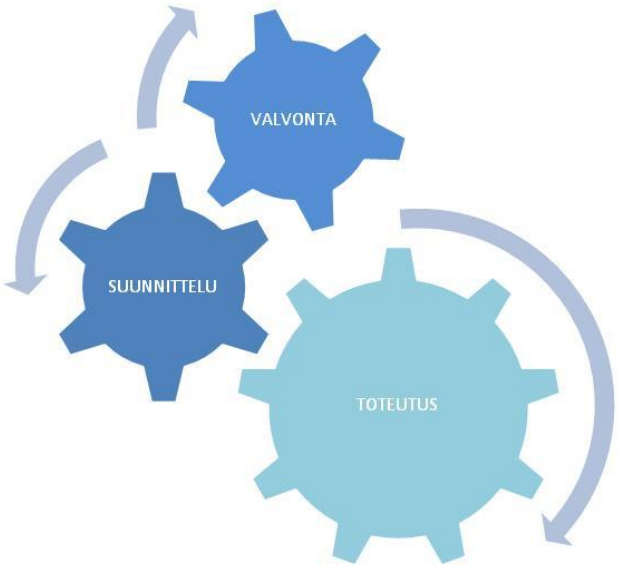
taan ja toiminnan koordinointiin. Resurssien tarve tulee huomioida jo suunnitteluvaiheessa.

5.4 Alihankkijoiden käyttö

Ulkoistetun palvelun tuottaja voi käyttää palvelun tuottamiseen alihankkijoita, ellei tätä ole erikseen kielletty. Kilpailutusvaiheessa tulisi pyytää tieto siitä, tullaanko palvelun tuottamisessa käyttämään alihankkijoita. Alihankkija voi tuottaa palvelua myös Suomen ulkopuolelta, ellei mahdollisuutta tuottaa palvelua Suomen ulkopuolelta ole rajattu kilpailutuksessa pois. Hankinnassa tulee myös huolehtia siitä, että palvelun tuottamiseen mahdollisesti käytettävää alihankkijaa koskevat samat velvoitteet kuin varsinaista palvelun tuottajaa ja sopimuksessa olisi hyvä sopia, tuleeko mahdollisen alihankkijan käyttö hyväksyttää palvelun hankkijalla ennen kuin alihankkijaa voidaan käyttää. SIEM-järjestelmän ja siihen liittyvän palvelun osalta tulee sopia, mitä seurauksia on siitä, että toiminta ei vastaakaan sovittua tasoa.

6 SIEM-ratkaisun käyttöönotto

Tilaajaorganisaation tulee asettaa SIEM-ratkaisun käyttöönotolle selkeät tavoitteet, jos halutaan, että lopputulos on toimiva. Käyttöönotto kannattaa suunnitella huolella, projektoida ja toteuttaa vaiheittain. Kunkin vaiheen lopuksi varmistutaan siitä, että saavutettiin kyseiselle vaiheelle asetetut tavoitteet ennen kuin siirrytään seuraavaan toteutusvaiheeseen. Käyttöönottoon tulee varata riittävästi aikaa ja resursseja.



Kuva 8. SIEM-ratkaisun käyttöönotto

Käyttöönottosuunnitelmassa ja siihen liittyvissä dokumenteissa tulee määritellä mm. missä vaiheessa ja millä aikataululla kukin järjestelmä liitetään SIEM-järjestelmään, miten liitettävät laitteet ja lokit konfiguroidaan, mitkä toiminnot SIEM-järjestelmässä otetaan käyttöön missäkin vaiheessa, mitä asiakkaan tarpeiden mukaisia muutoksia järjestelmään tehdään ja mitä raportteja, hälytyksiä yms. missäkin vaiheessa tuotetaan. Käyttöönottosuunnitelmassa kuvataan myös kunkin vaiheen aikataulutus, seuranta, dokumentointi sekä vaiheen lopputulosten hyväksyminen. Suunnitelmassa kuvataan myös käyttöönoton vaatimat resurssit sekä mistä ne saadaan. Toteutuksen onnistuminen varmistetaan kunkin vaiheen lopuksi testaamalla.

6.1 Vastuiden ja valtuuksien määrittely sekä valvonta

Käyttöönoton onnistumisen kannalta on tärkeää, että käyttöönottoon liittyvät vastuut on kuvattu riittävän tarkalla tasolla. Kaikkien osapuolten tulee olla selvillä siitä, kuka voi ottaa kantaa käyttöönotossa vastaan tuleviin asioihin ja tehdä tarvittavat päätökset. Mikäli vastuita ja valtuuksia ei ole määritelty riittävän tarkasti, tarvittavien päätösten saaminen voi kestää pitkään ja puuttuvat päätökset voivat estää käyttöönoton etenemisen sovitussa aikataulussa.

Palvelun tuottajan kanssa on sovittava, miten palvelun käyttöönoton edistymistä valvotaan. Valvontaan liittyy sekä palvelun tuottajan itse suorittama tai hankkima valvonta

sekä palvelun ostajan suorittama valvonta. Valvonnan tarkoituksen on varmistua siitä, että käyttöönotto saavuttaa sille asetetut tavoitteet ja mahdolliset käyttöönottoa haittaavat tai hidastavat asiat tunnistetaan mahdollisimman nopeasti, ja ne saadaan ratkaistuksi käyttöönoton vaatimassa aikataulussa.

6.2 Tekninen toteutuksen hyväksyminen

Käyttöönottovaiheen hyväksymisen yhteydessä tulisi teknisen toteutuksen osalta tarkistaa vähintään, että

- kaikki vaiheessa järjestelmään liitetyiksi suunnitellut laitteet on todistettavasti saatu liitetyksi järjestelmän piiriin. Mikäli jotain laitetta ei ole saatu liitetyksi järjestelmään, on selvitetty miksi liittäminen ei onnistunut ja sovittu liittämiselle uusi aikataulu.
- kaikista järjestelmään liitetyistä laitteista syntyy keskitettyyn lokien hallintajärjestelmään siirtyvää lokia.
- keskitettyyn lokien hallintajärjestelmään liitettyjen laitteiden lokien asetukset on tarkistettu ja todettu olevan sellaisia, ettei lokien keräys pysähdy esimerkiksi lokin täyttymiseen.
- toteutetut lokien asetukset on dokumentoitu, myös lokien asetuksiin tarvitut poikkeamat.
- toteutetut SIEM-järjestelmän asetukset on dokumentoitu.
- toteutuksen toiminta on testattu sekä lokien keräyksen että analytiikan, hälytysten ja raporttien osalta.
- tehdyt tarkistukset ja testaukset ovat asianmukaisesti dokumentoituja.
- jokaisesta SIEM-järjestelmään liitetystä laitteesta syntyy jokin merkintä esimerkiksi jollekin raportille, jotta voidaan todeta, että ko. laitteesta siirtyy dataa SIEM-järjestelmään.
- tuotetuilla raporteilla näkyvät kaikki ne tapahtumat, joiden pitäisi näkyä ja siinä muodossa kuin niiden pitäisi näkyä.
- lokien säilytysajat on määritelty ja niiden mukaiset siivousrutiinit on toteutettu.
- tarvittavat tietoliikenneyhteydet on toteutettu mahdollisimman pienin mutta riittävin tietoliikenneavauksin.

SIEM-järjestelmän, kuten kaikkien muidenkin järjestelmien, teknisen toteutuksen toimivuudesta tulee voida varmistua ennen käyttöönoton hyväksymistä. Järjestelmän toimivuudesta voidaan varmistua suorittamalla sille hyväksymistestaus, jota varten laaditaan

riittävän kattava testaussuunnitelma sekä siihen liittyvät testitapaukset. Testauksen perusteella avulla tulee voida varmistua, että tekninen toteutus vastaa kaikkia sille asetettuja vaatimuksia. Hyväksymistestauksen toteuttamisesta tulee pitää pöytäkirjaa.

6.3 Käyttöönoton dokumentointi

SIEM-järjestelmän käyttöönotto tulee dokumentoida riittävällä tasolla. Dokumentoinnista tulee käydä ilmi vähintään järjestelmän tekninen toteutus, mitkä laitteet on liitetty järjestelmän piiriin ja missä vaiheessa, mitkä olivat tarvittavat asetukset, miten lokit siirretään SIEM-järjestelmään ja miten toiminnan oikeellisuudesta on varmistuttu. Käyttöönoton yhteydessä tehdyn käyttöönottotestauksen suunnitelmat ja testauksen toteutuksen pöytäkirjat tulee liittää mukaan käyttöönoton dokumentteihin. Dokumentoinnin tulisi kattaa myös esimerkiksi, mitä analytiikkaa, hälytyksiä tai raportteja järjestelmään on konfiguroitu sekä mitkä laitteet ovat kunkin analytiikan, hälytyksen tai raportin piirissä.

7 Palvelun tuottajan kanssa sovittavia asioita

Palvelun hankkiminen ulkoistettuna palveluna tarkoittaa, että jokaisesta asiasta on hyvä sopia kirjallisesti. Jokaisella sovitulla asialla on myös kustannusvaikutuksia. Siksi palvelun käyttötarkoitus, tekninen toteutus, käyttöönotto ja varsinainen käyttäminen kannattaa suunnitella huolella. Palveluntuottajan kanssa on tarpeen sopia sekä palvelun tuottamisesta että myös siitä, miten toimintaa valvotaan sekä miten erilaisissa häiriö- tai poikkeamatilanteissa toimitaan, millaisia toimintaohjeita tarvitaan normaalia toimintaa varten, miten tuotettava palvelu on dokumentoitava, miten tarvittavat muutokset hoidetaan ja miten palvelua on tarkoitus jatkossa kehittää.

7.1 Vastuiden ja valtuuksien määrittely,

Palvelun mahdollisimman häiriöttömän tuotannon ja tulevan kehittämisen mahdollistamiseksi palvelun tuottamiseen liittyvät vastuut ja valtuudet on määriteltävä riittävän tarkasti ja selkeästi. Kaikkien osapuolten tulee tietää, kuka omistaa järjestelmän ja sillä tuotettavan palvelun sekä tilaajan että palvelun tuottajan organisaatioiden osalta. Vastuiden ja valtuuksien lisäksi kannattaa kiinnittää riittävästi huomiota osapuolten väli-

seen tiedonkulkuun, jotta vastaan tulevat ongelmien ratkaisut eivät viivästy puutteellisen tiedon kulun vuoksi.

Palvelun tuottamisen turvallisuuteen liittyvät velvoitteet on hyvä kirjata turvallisuussopimukseen. Turvallisuussopimuksen laatimisen apuna voidaan käyttää esimerkiksi Vahti-ohjeiden turvallisuussopimusmallia. [6.]

7.2 Palvelun tuottamiseen liittyvä valvonta

Palvelun tuottajan kanssa on sovittava, miten palvelun tuottamista valvotaan. Valvonta koostuu sekä palvelun tuottajan itse suorittamasta valvonnasta sekä palvelun ostajan suorittamasta valvonnasta. Valvonnan avulla voidaan varmistua siitä, että palvelua tuotetaan sopimuksen mukaisella tavalla. Lisäksi valvonnan tavoitteena on havaita vähintäänkin järjestelmään sovitun muutoshallinnan ohi tehdyt muutokset, käyttöoikeuksien ylitykset sekä muut poikkeamat palvelussa.

7.2.1 Palvelun ostajan suorittama valvonta

Palvelun ostajan suorittama palvelun valvonta perustuu joko tilaajaorganisaation suoraan järjestelmästä ottamiin raportteihin tai palvelun tuottajan toimittamiin tietoihin. Valvonnan tarpeisiin voidaan tuottaa esimerkiksi seuraavia raportteja:

- raportti järjestelmään raportointijakson aikana tehdyistä muutoksista
- raportti henkilöistä, jotka ovat katselleet lokien sisältöä raportointijakson aikana
- raportti henkilöistä, jotka ovat katselleet lokeista tuotettujen raporttien sisältöä jakson aikana
- raportti käyttöoikeuksien käytöstä jakson aikana
- raportti käyttöoikeuksista ja niihin jakson aikana tehdyistä muutoksista
- raportti keskitettyyn lokien hallintajärjestelmään siirrettyjen lokien määrästä
- raportti palvelun käyttökatkojen ja häiriöiden määrästä ja kestosta jakson aikana
- raportti ohjelmistojen ajantasaisuudesta

- raportti järjestelmästä jakson aikana poistetuista lokeista
- raportti havaituista poikkeamista
- raportti palvelutasovaatimusten täyttymisestä.

Yllä mainittujen raporttien listaus on esimerkinomainen ja tarvittavat raportit sekä niiden tarkkuus tulee sopia palvelun tuottajan kanssa sellaiselle tasolle, että palvelun luotettavuutta voidaan pitää riittävänä.

7.2.2 Palveluntuottajalta edellytettävä valvonta

Palvelun tuottajalta tulee edellyttää, että järjestelmää valvotaan sellaisella tavalla, että mahdolliset häiriöt palvelussa havaintaan mahdollisimman nopeasti ja tarvittavat korjaavat toimenpiteet käynnistetään ilman turhaa viivytystä.

Palveluntuottajan tulisi myös tekemänsä valvonnan perusteella havaita, mikäli keräyksen piirissä oleviin laitteisiin tehdään sellaisia muutoksia, että ne vaikuttavat lokien keräykseen tai niistä tuotettavaan tietoon, esimerkiksi siten, että lokeja ei enää siirry järjestelmään tai laitteista ei enää esimerkiksi synny merkintöjä raporteille. Palvelun tuottajan tulisi myös havaita, mikäli palveluun siirtyy lokeja sellaisista laitteista, joiden ei pitäisi olla keräyksen piirissä. Tällainen tilanne voi syntyä esimerkiksi silloin, kun laite korvataan uudella laitteella ja vanha laite otetaan eri käyttöön kuin aiemmin eikä laitteen SIEM-kytköksiä ole poistettu syystä tai toisesta.

Palvelun tuottaja tulee valvoa että SIEM-järjestelmään siirrettäväksi sovitut lokit siirtyvät keskitettyyn lokienhallintajärjestelmään ja ettei siirrossa ole häiriöitä tai katkoksia. Palvelun tuottajan tulisi myös valvoa, että raportit ovat ostajaorganisaation saatavilla sovittuna aikana ja sovitulla tavalla. Palvelun tuottajan tulisi myös valvoa mm. raporttien eheyttä ja laatua sekä hälytysten toimivuutta.

Palvelun tuottajan tulee valvoa, että palvelun tuottamiseen osallistuvalla henkilöstöllä on työtehtävien mukaiset henkilökohtaiset käyttöoikeudet SIEM-järjestelmään ja ettei sellaisilla henkilöillä, joiden työtehtäviin palvelun tuottaminen ei kuulu, ole käyttöoikeuksia järjestelmään. Palvelun tuottajan tulee huolehtia siitä, että käyttöoikeudet eivät ole liian laajat. Jos henkilö vaihtaa tehtäviä, työpaikkaa tai jää vaikkapa eläkkeelle, käyttöoikeudet tulee viivytyksettä päivittää vastaamaan muuttunutta tilannetta. Käyttö-

oikeuksien hallinnan tulisi olla mahdollisimman automaattista, jotta oikeudet saadaan tarvittaessa nopeasti poistetuksi useastakin järjestelmästä. Palvelun tuottajan tulee lisäksi valvoa sitä, että käyttöoikeuksia käytetään työtehtävien mukaisesti.

Palvelun tuottajan tulee myös osana suorittamaansa valvontaa raportoida tilaajalle havaitsemansa poikkeamat palvelussa.

7.3 SIEM-ratkaisuun liitettyjen järjestelmien valvonta

SIEM-ratkaisun avulla voidaan valvoa siihen liitettyjen järjestelmien toimintaa sekä havaita häiriöitä ja poikkeamia niiden toiminnassa. Valvonnan toteuttaminen riittävällä tasolla vaatii myös osaavaa henkilökuntaa, joka kykenee tunnistamaan häiriö- ja poikkeamatilanteita sekä toimimaan niiden vaatimalla tavalla. Mikäli tilaajaorganisaatio ei huolehdi tästä tehtävästä itse, sen tulee sopia palvelun tuottajan kanssa tarvittavien resurssien hankkimisesta.

7.4 Toimintaohjeet

Palvelun sujuvaa tuottamista varten tarvitaan toimintaohjeita sekä normaaliin toimintaan liittyen mutta myös erilaisten häiriö- ja poikkeamatilanteiden selvittämiseksi sekä mahdollisten tietoturva- ja tietosuojaloukkausten varalle. Etenkin häiriö- ja poikkeamatilanteissa toiminnan nopeus on ratkaisevaa lopputuloksen kannalta. Nopea ja laadukas toiminta vaatii etukäteen laaditut ja jalkautetut ohjeet. Ohjeiden toimivuutta ja ajantasaisuutta on tarpeen käydä läpi säännöllisesti ja tehdä niihin tarkastelun perusteella havaitut korjaukset.

7.4.1 Normaalin toiminnan ohjeistus

Palvelun normaalia toimintaa varten tulee määritellä toimintaohjeet, joiden avulla järjestelmän normaalin toiminnan tarpeet saadaan täytetyksi siten, että myös palvelulle asetetut turvallisuuteen liittyvät vaatimukset täyttyvät. Toimintaohjeissa kuvataan myös esimerkiksi, keneltä pyyntö voi tulla, miten pyyntö hyväksytään tai hylätään ja millä tavoin ja minne pyyntö tulee dokumentoida. Ohjeissa kuvataan myös normaaliin toimintaan liittyvä viestintä.

Toimintaohjeita tarvitaan esimerkiksi seuraavien tapahtumien hoitamiseksi

- uuden laitteen lisääminen
- vanhan laitteen poistaminen
- olemassa olevan laitteen korvaaminen uudella laitteella
- uuden säännöllisen raportin tilaaminen ja tuottaminen
- olemassa olevan raportin muokkaaminen
- lisäraporttien tilaaminen
- uuden hälytyksen tilaaminen
- vanhan hälytyksen poistaminen
- olemassa olevan hälytyksen muokkaaminen
- käyttöoikeuksien hallinnointi
- säilytysaikojen muuttaminen.

Edellä olevassa listassa on esimerkkejä yleisimmistä tilanteista, mutta normaali toiminta vaatii myös muita ohjeita.

7.4.2 Poikkeama- ja häiriötilanteiden ohjeistus

Palvelun mahdollisimman häiriöttömän toiminnan varmistamiseksi tulee huolehtia siitä, että vähintään yleisimpien häiriöiden ja poikkeamatilanteiden varalle on luotuna asianmukaiset, toimivat prosessit. Prosesseja luotaessa tulee myös varmistaa, että reagointiin mahdollisesti tarvittavat lisävaltuudet ovat saatavissa, myös normaalin työajan ulkopuolella.

Huomioitavia häiriötilanteita voivat olla esimerkiksi ennakoimaton katkos yksittäisen tai useamman lokin tuottamisessa tai siirtämisessä SIEM-järjestelmään tai muu järjestelmän toiminnan häiriintyminen. Häiriötilanteen sattuessa palvelun tuottajan tulee tietää, miten ja missä ajassa tilanteessa tulee toimia ja miten, milloin ja kenelle tapahtuneesta pitää raportoida sekä palvelua tuottavassa organisaatiossa että tilaajaorganisaatiossa ja miten tapahtuma tulee dokumentoida.

Palveluntuottajan tulee myös kyetä tunnistamaan vähintäänkin ennakolta kiinnostavaksi määriteltyjä poikkeamatilanteita sekä tietää, miten tilanteissa pitäisi toimia ja missä ajassa.

7.4.3 Tietoturva- ja tietosuojaloukkaustilanteiden ohjeistus

SIEM-järjestelmään kerätyn tiedon käsittelyn yhteydessä voidaan päätyä esimerkiksi tilanteeseen, jossa paljastetaan tahattomasti luottamuksellista tietoa. Yksi esimerkki tällaisesta tilanteesta on käyttäjien käyttäjätunnus-salasana-yhdistelmän paljastuminen epäonnistuneiden kirjautumisten raportin kautta. Luottamuksellisten tietojen tahattoman tai tahallisen paljastumisen varalle tulee olla ohjeet, miten tilanteessa menetellään, esimerkiksi miten tilanteesta tiedotetaan henkilölle, jonka luottamuksellisia tietoja on paljastunut ja mihin muihin toimenpiteisiin tilanteessa tulee ryhtyä.

7.5 Muutosten hallinta

Käyttöönoton yhteydessä todennäköisesti toteutetaan ensimmäinen vaihe SIEM-järjestelmän käyttöönotosta ja jätetään joitakin ominaisuuksia toteutettavaksi myöhemmin. Käyttöönoton jälkeen itse järjestelmään tai sen avulla tuotettavaan palveluun on tarpeen tehdä muutoksia esimerkiksi tekniikan kehittyessä tai käytön laajentuessa. Vähintäänkin palvelun piirin liitettyjen laitteiden ja lokien määrät voivat muuttua ajan myötä. Liitettyjen järjestelmien käyttöjärjestelmät voivat muuttua tai järjestelmään halutaan viedä uuden tyyppisiä sovelluslokeja. Järjestelmään liittyvien käyttöoikeuksien laajuus voi muuttua.

Muutosten hallintaa varten tulee mm. määritellä, miten muutosten vaikutusten arviointi tehdään, miten muutosten hyväksyntä tai hylkääminen tapahtuu, miten muutoksen toteutuksen onnistuminen varmistetaan, miten muutosten aikatauluista sovitaan ja miten muutoksesta tiedottaminen hoidetaan. Muutosten hallinnan yhteydessä tulee huolehtia siitä, että järjestelmään tehtävät muutokset pystytään todentamaan myös jälkikäteen.

7.6 Tekninen toteutus ja palvelutaso

Hankittavan SIEM-järjestelmän teknistä toteutusta on määritelty jo hankintavaiheessa. Käyttöönoton yhteydessä on päätetty esimerkiksi lokien keräykseen tarvittavista tietoliikenneavauksista, keräykseen käytettäville käyttäjätunnuksille asetettavista vaatimuksista, lokien säilytysajoista, lokien poistamisesta sekä muista teknisistä yksityiskohdista. Järjestelmän peruskäyttötarkoitus eli kaikkien keräyksen piirissä olevien lokien kerääminen talteen mahdollista myöhempää käyttöä varten edellyttää, että palvelu lokien keräyksen ja tallentamisen osalta on käytössä koko ajan ilman katkoja. Teknisen toteutuksen tuleekin olla sellainen, ettei katkoja synny esimerkiksi järjestelmän perusylläpidon vuoksi.

Tuotetulle palvelulle määritellään palvelutasovaatimukset, joiden toteutumista seurataan. Palvelutasovaatimuksissa määritellään muun muassa, kuinka nopeasti pyydetyt muutokset tulee toteuttaa, missä ajassa poikkeamiin tai häiriötilanteisiin pitää reagoida.

7.7 Palvelun dokumentointi

Palvelun jatkuvan toiminnan tulee olla kattavasti dokumentoitua. Varsinainen palvelu, tekninen toteutus ja käyttöönotto sekä uudet toiminnallisuudet, järjestelmään tehdyt muutokset, järjestelmän ominaisuudet ja järjestelmän tarjoamat jatkokehitysmahdollisuudet tulee dokumentoida siinä muodossa, että niitä voidaan käyttää esimerkiksi järjestelmän kehittämisen pohjana. Palvelua kuvaavien dokumenttien ylläpidosta tulee huolehtia siten, että niistä on aina saatavilla ajantasainen versio.

Palvelun tuottajan tulee tehdä SIEM-järjestelmästä asiakaskohtainen dokumentti, jossa kuvataan paitsi asiakkaalle tehdyn ratkaisun tekninen toteutus, myös mitkä laitteet ja niillä olevat lokit on liitetty keräyksen piiriin sekä mitä tunnuksia keräykseen käytetään. Dokumentissa tulee kuvata myös esimerkiksi, mitä analytiikkaa, hälytyksiä ja raportteja järjestelmään on rakennettu sekä niiden ja palveluun liitettyjen laitteiden ja lokien väliset kytkökset.

Dokumenteissa kuvataan mm. järjestelmän oikean toiminnan varmistamiseksi toteutetut kontrollit sekä miten palvelun tuottamista valvotaan. Osapuolten palvelun tuottami-

seen liittyvät vastuut ja valtuudet tulee myös olla selvillä ja niiden tulee olla dokumentoituina. Myös palvelun sisällön tulee olla dokumentoitu riittävän tarkasti.

7.8 SIEM-ratkaisun kehittäminen

SIEM-järjestelmän toimittajalla tulee olla näkemys siitä, miten järjestelmän teknisen toteutuksen ja siihen liittyvien ohjelmistojen ajantasaisena pysymisestä huolehditaan. Laitteiston ikääntyessä sen korvaaminen uudella tulee suunnitella hyvissä ajoin. Järjestelmän toimittajan tulee osata kertoa, mitä uusia ominaisuuksia järjestelmään on saatavilla sekä miten ja millä aikataululla niiden käyttöönotto on mahdollista. Toimittajan tulee osata kertoa, minkälaisia lokeja tuottavia laitteita on mahdollista liittää keskitetyn lokien keräyksen piiriin.

8 Tilaajaorganisaation tehtäviä

Vaikka palvelu ostettaisiin pääosin ulkopuolisen tuottamana, tilaajaorganisaation tulee huolehtia siitä, että palvelu vastaa sille asetettuja tavoitteita. Tilaajaorganisaatiossa tulee olla määriteltynä, kuka tai mikä taho viime kädessä vastaa SIEM-palvelun toiminnasta tilaajaorganisaatiossa. Vaikka viimeinen hyväksyntä palveluun liittyville merkittäville linjauksille haettaisiinkin esimerkiksi johtoryhmästä, toteuttavalle portaalle tulee määritellä sellainen vastuutaho, joka voi käyttää päätäntävaltaa tavallisemmissa SIEM-ratkaisuun liittyvissä asioissa. Tämä taho vastaa esimerkiksi siitä, että

- palvelulle on nimetty omistaja.
- SIEM-palvelun valvonta kokonaisuudessaan on tilaajaorganisaation kannalta riittävällä tasolla.
- palveluun liittyvät vastuut ja valtuudet on dokumentoitu.
- tilaajaorganisaatio on määritellyt SIEM-palveluun liittyvän aineiston käsittelyohjeet ja niihin liittyvät prosessit.
- periaatteet, joiden mukaisesti voidaan antaa käyttöoikeuksia SIEM-järjestelmään ja sen tuottamaan materiaaliin, ovat olemassa.
- tarvittavat toimintaohjeet häiriö- ja poikkeamatilanteita varten ovat luotuina.
- tarvittavat prosessit ovat luotuina.

- muutosten hallintaa varten ovat olemassa tarvittavat prosessit ja ohjeistus.
- dokumentit ovat ajantasaisia.
- tarvittavat rekisteriselosteet on tehty.
- käsittelyn mahdollisesti vaatimat yt-prosessit on hoidettu asianmukaisesti.

SIEM-palvelun vastuutaho huolehtii siitä, että palvelun häiriöttömälle toiminnalle on olemassa edellytykset ja poikkeavista tilanteista palataan takaisin normaaliin tilanteeseen mahdollisimman nopeasti ja pienin vahingoin.

8.1 Valvonta

Jotta voidaan olla varmoja siitä, että palvelua tuotetaan sovitulla tavalla, tilaajan tulee valvoa palvelun tuottamista. Tilaajalla on myös vastuu palveluun liitettyjen järjestelmien toiminnasta. Tilaajaorganisaation on tarpeen varata resursseja sekä tuotettavan palvelun että siihen liitettyjen järjestelmien toiminnan valvomiseksi. Valvontaa suorittavalla henkilöstöllä tulee olla riittävä osaaminen tehtäviinsä nähden. SIEM-palvelussa voi olla liitettynä monta tilaajaorganisaation järjestelmää, joten tilaajaorganisaatiossa on hyvä sopia mitkä asiat valvotaan keskitetysti ja mitkä valvontatehtävät kuuluvat esimerkiksi kunkin järjestelmän omistajan tehtäviin.

8.2 Tilaajaorganisaation toimintaohjeet ja prosessit

Palvelun jatkuvan toiminnan varmistamiseksi tilaajalla tulee olla ohjeet ja prosessit paitsi häiriö- ja poikkeamatilanteiden varalle niin myös normaalin toiminnan toistuvien tapahtumien hoitamiseksi. Prosessien ja ohjeiden ajantasaisuus tulee varmistaa säännöllisellä katselmoinnilla.

8.2.1 Normaalin toiminnan ohjeistus

Palvelun toimiessa normaalisti palveluun halutaan todennäköisesti liittää uusia järjestelmiä tai poistaa siitä vanhoja järjestelmiä. SIEM-palveluun liitettäville laitteille halutaan uusia hälytyksiä tai raportoinnin tarve voi muuttua. Tuotettuja raportteja tulkitaan ja niiden avulla muodostetaan kokonaiskuvaa SIEM-palveluun liitettyjen järjestelmien

tilanteesta. Palvelua tuottava henkilöstö voi vaihtua sekä tilaavassa että palvelua tuottavassa organisaatiossa ja uudet henkilöt pitää saada hyväksytyiksi tuottamaan palvelua ja heille pitää saada työtehtäviä vastaavat käyttöoikeudet. Näiden normaalissa toiminnassa vastaan tulevien tilanteiden osalta tulee olla kirjallinen ohjeistus, miten tilaajaorganisaatiossa kussakin tilanteessa tulee toimia.

8.2.2 Häiriö- ja poikkeamatilanteiden ohjeistus

Tilaajaorganisaation on tarpeen määritellä, miten toimitaan esimerkiksi tilanteessa, jossa kerättyjen lokien pohjalta muodostetun raportin perusteella voidaan olettaa, että asiaa on tarpeellista tutkia lisää. Näitä tilanteita varten on tarpeen määritellä, kuka tai mikä taho voi tehdä lisätutkimuksia asiaan liittyen ja minne ja miten tutkinnassa syntynyt tieto tallennetaan ja miten tutkinta dokumentoidaan. Hälytysten tai muiden nopeaa reagointia vaativien tapahtumien varalle tulee sopia edellä mainittujen asioiden lisäksi, miten toimitaan, jos reagointia vaaditaan myös normaalin työajan ulkopuolella. Lisäksi on hyvä ohjeistaa ennalta, miten toimitaan, jos tapahtuman selvittämiseen tarvitaan ulkopuolista apua. Tilaajaorganisaation tulee myös määritellä palvelun tuottajaa varten ennakolta kiinnostaviksi tunnistettuja poikkeamia, joihin palvelun tuottajan organisaation on reagoitava ennalta sovitulla tavalla ja sovitussa ajassa.

8.2.3 Tietoturva- ja tietosuojaloukkaustilanteiden ohjeistus

Myös tilaajaorganisaatiolla tulee olla ohjeistus siitä, miten toimitaan, mikäli päädytään tilanteeseen, jossa paljastuu tahattomasti tai tahallisesti luottamuksellista tietoa. Tilaajaorganisaatiossa tulee olla tiedossa, kenelle tapahtuneesta ilmoitetaan ja mihin toimenpiteisiin tapahtuneen johdosta tulee ryhtyä. Toimenpiteet tulee osata suorittaa riippumatta siitä, kuka tilanteen havaitsee ensimmäisenä.

8.3 Muutosten hallinta

Ajan kuluessa tuotettavaan SIEM-palveluun tarvitaan erilaisia muutoksia. Esimerkiksi palvelun tuottamistapaan voidaan tarvita muutoksia tai laitteistoa joudutaan uusimaan tai vaihtamaan. Suunnitelluilla muutoksilla voi olla merkitystä vain osalle SIEM-ratkaisuun liitetyistä järjestelmistä tai muutoksilla voi olla vaikutusta palveluihin, joita tuotetaan kaikille SIEM-ratkaisuun liitetyille järjestelmille. Muutoksia kuitenkin tulee ja

niitä varten myös tilaajaorganisaatiossa tulee olla suunniteltuna prosessit, joiden avulla arvioidaan muutoksen tarve ja vaikutus ja joiden mukaisesti tarpeellisiksi arvioidut muutokset saadaan toteutettua.

8.4 Palvelun kehittäminen

Palvelun käyttöönoton yhteydessä otetaan usein ensin käyttöön vain osa SIEM-palveluun kuuluvista toiminnoista ja osan toteutus siirretään myöhempään ajankohtaan. Kokemuksen karttuessa toimintaa on todennäköisesti tarpeen kehittää vastaamaan vielä paremmin tilaajaorganisaation tarpeita. Pian käyttöönoton jälkeen onkin tarpeellista nimetä vastuuhenkilö SIEM-palvelun kehittämiselle.

9 Yhteenveto

Työssä ei pyritty saamaan aikaan täydellistä listaa siitä, mitä kaikkea palvelun ulkoistajan tulee huomioida mutta työn avulla ostajalla on paremmat mahdollisuudet hahmottaa asiaan liittyvä kokonaisuus. Lopputyön tuloksena syntyi dokumentti, jota ulkoistetun SIEM-ratkaisun hankkija voi käyttää apunaan sekä tarvittavan ratkaisun määrittelyssä että hankittavan kokonaisuuden hahmottamisessa. Vaikka SIEM-ratkaisu hankitaan ulkoistettuna palveluna, kaikkea ei voi ulkoistaa, vaan myös tilaajaorganisaatiolle jää tehtäviä hoidettavaksi.

Onnistunut lopputulos vaatii paljon valmistelevaa työtä. SIEM-ratkaisun hankinnan käyttötarkoitus on suunniteltava huolella ja järjestelmälle ja sen käytölle asetettavat vaatimukset kannattaa määritellä riittävän tarkasti. Järjestelmän käytön tulee vastata organisaation liiketoiminnan tarpeita ja tehtävien määrittelyjen ja vaatimusten tulee lähteä liiketoiminnan tarpeista.

Toimivan ratkaisun aikaansaaminen vaatii jatkuvaa keskustelua eri yhteistyötahojen kesken eikä keskustelua saa tai voi lopettaa siihen, kun järjestelmä on asennettu. Toimivan järjestelmän rakentaminen vaatii keskustelujen lisäksi myös aikaa ja valmiutta tarkastella aiemmin tehtyjä valintoja uudelleen järjestelmän toiminnan ja toteutuksen kehittyessä.

Toteutukseen kannattaa varata riittävästi resursseja paitsi varsinaiseen hankintaan ja käyttöönottoon mutta myös itse järjestelmän hyödyntämiseen sitten, kun se on jo käytössä. Ratkaisun käyttöönotto kannattaa toteuttaa vaiheittain ja siirtyä seuraavaan vaiheeseen vasta, kun edellinen vaihe on saatu toteutettua hyväksytysti. Tarvittavien prosessien luominen vaatii myös aikaa, osaamista sekä resursseja ja ne tulisi luoda riittävän varhaisessa vaiheessa hankintaprosessia.

Palvelun toimittajalla on käytössään sekä myynnin että tekniikan asiantuntijat, palvelun hankkijan kannattaa myös hankkia itselleen tueksi tekninen osaaja tai esim. asiaan perehtynyt konsultti.

Lähteet

1 KPMG Oy Ab: Unkown Threat in Finland. Viitattu 15.1.2014. http://www.kpmg.com/FI/fi/Ajankohtaista/Uutisia-ja-julkaisuja/Neuvontapalvelut/Documents/unknown-threat-in-finland.pdf.

2 Mandiant: APT1 Exposing One of China's Cyber Espionage Units. Viitattu 26.3.2014. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

3 Malvare.lu: APt1 Technical backstage. Viitattu 26.3.2014. http://www.malware.lu/Pro/RAP002_APT1_Technical_backstage.1.0.pdf.

4 Ponemon institute: 2013 Cost of Data Breach Study: Global Analysis. Viitattu 6.4.2014. http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf.

5 VAHTI 3/2009 Lokiohje. Viitattu 1.1.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf.

6 VAHTI-turvallisuussopimusmalli. Viitattu 25.3. 2014. https://www.vahtiohje.fi/c/document_library/get_file?uuid=889c293a-2650-444c-8fea-51434dcc7f6e&groupId=10128.

7 Nixu Tiger Team Blogi: Malware.lu-sivuston raportti APT1-hyökkäyksestä. Luettu 11.3.2014. http://www.nixu.com/fi/blogi/2013-04/malwarelu-sivuston-raportti-apt1-hy%C3%B6kk%C3%A4yksest%C3%A4.

8 Scott Gordon, CISSP: Operationalizing Information Security Putting the Top 10 SIEM Best Practices to Work (2010). Luettu 10.3.2014. http://www.eslared.org.ve/walcs/walc2012/material/track4/Monitoreo/Top_10_SIEM_Best_Practices.pdf.

9 David Swift: Successful SIEM and Log Management: Strategies for Audit and Compliance (2010). Luettu 16.3.2014. https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528.

10 J. Michael Butler: Benchmarking Security Information Event Management (SIEM). A SANS Whitepaper – February 2009. Luettu 6.4.2014. http://www.sans.org/reading-room/analysts-program/eventMgt-Feb09.

11 RQ News & Blog: Four Points to Successfully Research SIEM Solutions. Luettu 6.4.2014. http://www.reliaquest.com/four-points-to-successfully-research-siem-solutions/.

12 Solarwinds: Log & Security Information Management. Luettu17.3.2014. http://www.solarwinds.com/siem-security-information-event-management-software.aspx.

13 Cygate:Tiedätkö mitä tietoverkossasi ja palveluissasi tapahtuu? Luettu 5.1.2014. http://www.cygategroup.com/upload/Finland/Palvelut_ja_ratkaisut/Tietoturva/Cygate_SIEM-ratkaisut.pdf.

14 McAfee:SIEM: Keeping Pace with Big Security Data. Luettu 17.3.2014. http://www.mcafee.com/us/resources/reports/rp-siem-keeping-pace-big-security-data.pdf.

15 Insta defSec: Kokemuksia SIEM-järjestelmistä. Luettu 17.3.2014. http://www.siemseminaari.fi/binary/file/-/id/1/fid/25.

16 TechRepublic: How to choose a SIEM solution: An overview. Luettu 17.3.2014. http://www.techrepublic.com/blog/it-security/how-to-choose-a-siem-solution-an-overview/.

17 Informationweek: IT Pro Ranking: SIEM. Luettu 6.4.2014. http://reports.informationweek.com/abstract/21/8901/security/it-pro-ranking-siem.html.

18 Kauppalehti: POHJOISRANTA BURSON-MARSTELLER OY: Tutkimus: Kyberrikollisuuden kustannukset nousseet 78 % neljässä vuodessa, hyökkäykset selviävät puolet aiempaa hitaammin. Luettu 6.4.2014. http://www.kauppalehti.fi/5/i/yritykset/lehdisto/cision/tiedote.jsp?selected=kaikki&oid=20131001/13812327437570.

19 Teemu Hyvärinen: Haavoittuvuusskannausten ja IDS-hälytyksien ristiinkorrelointi AlienVault OSSIM SIEM-järjestelmässä 2013. Luettu 15.2.2014. Viitattu 14.4.2014 https://www.theseus.fi/handle/10024/64116.

20 SIEM Guru 2012: What is SIEM vs. SIM vs. SEM. Luettu 15.2.2014. http://siemguru.com/index.php?option=com_easydiscuss&view=post&id=40.

21 Jamil, A. 2009. The difference between SEM, SIM and SIEM. Luettu 11.11.2013. Viitattu 14.4.2014. http://amirjamil.blogspot.fi/2009/07/difference-between-sem-sim-and-siem.html.

22 TechRepublic: A log review process for detecting security incidents. Viitattu 14.4.2014. http://www.techrepublic.com/blog/it-security/a-log-review-process-for-detecting-security-incidents/6601/.

23 The SANS Institute, 2006 Security Information/Event Management. Security Development Life Cycle Version 5. Luettu 15.2.2014. *https://www.sans.org/score/esa_current.doc*.

24 Dorigo, S. 2012. Security Information and Event Management. Luettu 1.03.2014. Viitattu 14.4.2014. http://www.ru.nl/publish/pages/578936/thesissanderdorigo.pdf.

Lokeihin liittyviä säädöksiä ja ohjeita

Lokien käsittelyyn kohdistuu lainsäädäntöön perustuvia vaatimuksia, mm seuraavista laeista ja asetuksista:

- Henkilötietolaki (523/1999)
- Julkisuuslaki (621/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004) (”työelämän tietosuojalaki”)
- Sähköisen viestinnän tietosuojalaki (526/2004)
- Yhteistoimintalaki (334/2007)
- Tietoturva-asetus (681/2010).

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI:n monissa julkaisuissa annetaan lokeihin liittyviä ohjeita. Tällaisia julkaisija ovat mm. seuraavat julkaisut:

- VAHTI 4/2013 Henkilöstön tietoturvaohje
- VAHTI 1/2013 Sovelluskehityksen tietoturvaohje
- VAHTI 3/2012 Teknisen ICT-ympäristön tietoturvataso-ohje
- VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta:
- VAHTI 3/2009 Lokiohje
- VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje.